AF/3621 #19 7-16-03 mel

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPELLANTS:	Rosenau et al.	CONFIRMATION NO. 8261
SERIAL NO.:	09/593,406	GROUP ART UNIT: 3621
FILED:	June 14, 2000	EXAMINER: K. Abdi
TITLE:	"ARRANGEMENT AND METHOD FOR GENERATING A SECURITY IMPRINT"	

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANTS' BRIEF ON APPEAL

S I R:

In accordance with the provisions of 37 C.F.R. §1.192, Appellants herewith submit their main brief in support of the appeal of the above-referenced application.

REAL PARTY IN INTEREST:

The real party in interest is the assignee of the application, Francotyp-Postalia AG & Co. KG, a German corporation.

RELATED APPEALS AND INTERFERENCES:

There are no related appeals and no related interferences.

STATUS OF CLAIMS:

The application was originally filed with claims 1-14 and no claim was cancelled during prosecution. All claims 1-14 are the subject of the present appeal.

STATUS OF AMENDMENTS:

No Amendment was filed following the final rejection dated February 3, 2003.

SUMMARY OF THE INVENTION:

The present invention concerns a method and arrangement for generating a security imprint within a print image that also contains other printed information, such as a franking imprint printed by a postage meter.

In general, processing time is reduced, and throughput of printed items is correspondingly increased, in accordance with the invention by undertaking two time-offset calculations in different computers. The calculation of the security code, which is needed to produce the security imprint, is undertaken in a security module, while editing of the other print image data, is undertaken by the processor which controls the printing arrangement. A high system clock performance is achieved by appropriate interleaving of these two tasks and specific selection of algorithms and data structures.

Figure 1a shows a time/control diagram for a postage meter machine that is equipped in a known way with a microprocessor that implements the following steps for generating security imprints when franking:

-- input routine 401 in order to set the postage value;

-- sensor routine 402 in order to identify the letter insertion, with

-- sub-routine 406-411 for DAC calculation;

-- request routine 403 for accounting, with

-- sub-routine 412, 413 for the accounting and with

-- sub-routine 414 for offering DAC;

-- calculation routine 404 for the print image; as well as

-- print routine 405. (p. 5, l. 11-21)

A data processing time duration Told per franking with a security imprint is required in the implementation of the individual routines and sub-routines due to the sequential processing. (p.6, l.1-3)

The inventive time/control diagram (shown in Figure 1b) for a postage meter machine requires a data processing time duration T_{new} per franking with a security imprint that is shorter than the old data processing time duration Told per franking. This is possible only because a division of tasks for two data processing units occurs in the invention, whereby a microprocessor is provided in the meter for the printing tasks and a security module is provided for the security tasks. (p.6, l.4-9)

The printing tasks include an input routine 401 in order to set the postage value, a sensor routine 402 in order to determine the insertion of a letter, a request routine 403 for accounting, a calculating routine 404 for the print image as well as a print routine 405. (p.6, l.10-12)

The security tasks include a sub-routine 406-411 for the DAC calculation, a sub-routine 412, 413 for the accounting and a sub-routine for offering the DAC. (p.6, l.12-13)

The calculating routine 404 for the print image is especially complicated for a security imprint, for which reason the formatting of the print image already begins before the end of the accounting. Moreover, the microprocessor in the meter implements the print routine 405, while the security module already calculates the security code the next print image as soon as a letter sensor senses that a further letter is pending at the input of the transport path. (p.6, l.14-19)

This is particularly meaningful given mass frankings of postal items, particularly letters, having the same postage value. The adjacency of a further letter

that is acquired at the input of the transport path by a letter sensor triggers an interrupt for the microprocessor in the meter, which reports the pending letter to the security module and then continues with the calculations that have been begun for formatting the print image. (p.6, l.20 – p. 7, l.4)

Inventively, the microprocessor stills works on formatting the print image (step 404) or is occupied with the implementation of the print routine (step 405) while the report 412 of a further letter pending ensues to the security module, whereupon the latter already implements further calculations 316-321 for a next piece of mail (letter). (p.7, l.7-10)

As soon as the microprocessor is finished with the implementation of the print routine (step 405), a request is made to the security module to implement an accounting. The security module now implements the accounting (steps 322, 323) and sends (step 324) the security code DAC to the microprocessor 91 of the meter, which is now in a position to complete the formatting of the print image for the further print image (step 414). (p.7, l.11-16)

Figure 3 shows a perspective view of the inventive postage meter machine from behind. The postage meter machine is composed of the meter 1 and of a base 2. The latter is equipped with the chip card write/read unit 70 that is arranged behind a guide plate 20 and is accessible from the upper edge 22 of the housing. After the postage meter machine is turned on with the switch 71, a chip card 49 is inserted into the insertion slot 72 from top to bottom. A letter 3 that is supplied standing on edge and that has its surface to be printed lying against the guide plate 20 is then printed with a security imprint 31 corresponding to the input data. The letter delivery opening is laterally limited by a transparent plate 21 and the guide plate 22. The

status display of the security module 100 plugged onto the motherboard 9 of the meter 1 is visible from the outside through an opening 109. (p.11, l.7-17)

A detailed block diagram showing the interior electrical components of the postage meter machine of Figure 3 is shown in Figure 2. It is not necessary to include a detailed explanation of the operation and interaction of all of those components, however, in order to understand the subject matter of the claims on appeal, and therefore such a discussion is not included herein. A complete discussion, however, appears in the original application, which can be consulted if necessary.

Figure 4 shows an illustration of a security imprint as required by the USPS. The security imprint is arranged to the right of the advertising slogan and includes the carrier logo and the postage value in the upper half and the date, the postage value, a key indicator and a data authentification code in a first line and a manufacturer ID, a machine ID, a model ID and the ascending register value in a second line in the lower half, whereby both lines are machine-readable. Both machine-readable lines are laterally limited by marking bars that improve the recognition and the interpretation of the characters according to an OCR method. A corresponding evaluation method for the aforementioned data that reproduce the characters is disclosed in European Application 862 143, corresponding to United States Patent No. 5,953,426 for checking a security imprint. (p.11, l.18 - p.12 l.5)

Inventively, the calculation of the DAC for the security imprint is implemented in the security module. A further speed-up in the calculation of the security code is achieved by the selection of an assembler algorithm that is specifically selected and certified for the DES calculation. In order to also be able to authenticate print data

that merely indicate parts of a date with an OCR read station, a "left-out value" is defined for these specific date values. This is employed instead of the date entry. For example, the value 0 is employed when the corresponding date parts are not present. (p. 12, l.6-12)

Storing the current date in two different formats and memory locations is necessary in order to check the print date for validity, since the format of the security modules internal real-time clock (RTC) differs from the format of the date employed in the print image and a comparison at the point in time of the accounting requires corresponding time. (p. 12, l.13-17)

The structure and the interpretation of the system data that enter into the security code, as well as the system data that are used by the FM for the printing enable a further speed-up. (p. 12, l.18-19)

Since the print date usually remains constant given mass frankings, the first 8 bytes of the security code can be calculated in advance for each day in a first 3DES routine. (p. 12, l.20-22)

Table 1 shows a further example for the data that proceed from a security imprint. (p.13, l. 1-15)

Table 1:

#	Information	Value Range		Left out Zeroes	Leading
1.		**Lower**	**Upper**		
2.	Date of mailing Month:	JAN	DEC	'---'	
3.	Day:	01	31	'--'	YES
4.	Year:	1999		'----'	
5.	Postage	00000	99999		YES
6.	Key indicator	0	9		
7.	Data authentication code	00000	65535		YES
8.	Vendor ID	FP			
9.	Machine ID	0000001	9999999		YES
10.	Model ID	JMB01	JMB99		
11.	Ascending register	00000000	FFFFFFFF		YES

Table 2 illustrates the length of the required bytes of individual and of all system data that enter into the calculation of the security code. (p.12, l.17-24)

Table 2:

	Element	Byte length	Value range (decimal)
1.	Machine ID	4	7-digit value range for Francotyp-Postalia
2.	OCR key indicator	1	0...9
3.	Mailing date Sub-elements: Year Month Day	Total: 3 Detail: 1 1 1	 0..99, 0..12, 0..31,
4.	Postage value	4	0..99999 (unit is 1/10 cents)
5.	Ascending register	4	0..4294967295 (unit is 1/10 cents)
	TOTAL:	**16**	

Table 3 shows and example of system data for a security code.

Table 3

	Serial number				K1	Mailing date			Postage value				Ascending register			
Decimal Data	0050010				1	Feb 17 1999			$12.300				$129.300			
Hex. Data	00	00	C3	5A	01	63	02	11	00	00	30	0C	00	1F	91	14

ISSUES:

The following issues are the subject of the present appeal:

Whether the subject matter of claims 1 and 9-11 would have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) based on the teachings of United States Patent No. 5,680, 463 (Windel et al. '463) and United States Patent No. 4,934,846 (Gilham) in view of United States Patent No. 6,418,422 (Guenther);

Whether the subject matter of claims 2-5, 12 and 13 would have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) based on the teachings of Windel et al. '463, Gilham and Guenther, further in view of United States Patent No. 4,649,266 (Eckert);

Whether the subject matter of claim 6 would have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) based on the teachings of Windel et al. '463, Gilham, Guenther and Eckert, further in view of United States Patent No. 5,671,146 (Windel et al. '146); and

Whether the subject matter of claims 7 and 8 would have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) as being unpatentable over Windel et al. '463, Gilham, Guenther, Eckert and Windel et al. '146, further in view of United States Patent No. 6,058,193 (Cordery).

GROUPING OF CLAIMS:

The patentability of claims 1-14 stands or falls together.

ARGUMENT:

As noted above, an important feature of the method and apparatus of the claims on appeal is the division of tasks between two data processing units, namely a security module for processing security tasks, and a microprocessor for processing printing tasks. This division of tasking (processing) results in a processing time duration per franking with a security imprint that is shorter then the processing time duration per franking which was achievable by conventional methods and systems, which did not employ such a processing division.

In the substantiation of the aforementioned rejection in the final rejection, the Examiner acknowledged that neither Windel et al '463 nor Gilham explicitly discusses the separate data processing for the franking imprint at the printing module. The Examiner stated it would have been an obvious matter of design choice to modify the teachings of Windel et al '463 and Gilham to provide separate data processing externally of the security module, because the Examiner stated that the Appellants have "not disclosed that additional data processing solves any stated problem in a new or unexpected way or is for any particular purpose which is unobvious to one of ordinary skill in the art ...". Appellants are unable to understand how the Examiner can make such a statement in view of the numerous explanations in the specification as to the significant advantages achieved by such separate data processing for security purposes and for printing purposes, including the passage cited in the "SUMMARY OF THE INVENTION" section herein, from page 6, lines 4-9 of the specification.

Windel et al '463 discloses a method and an arrangement for generating and checking a security imprint. The arrangement for generating the security imprint shown in Figure 1 of the Windel et al '463 reference does not disclose a security module with a data processing unit separate therefrom. The Gilham reference teaches a franking system having numerous embodiments, but none of those embodiments disclose a separate security module and a separate data processing unit.

The Examiner relied on the Guenther reference as teaching a "secondary" data processing unit external to the security module, the Examiner referring to a smart card as such a "secondary" data processing unit. While this is correct, the tasks of compiling a printing image and generating a security code in the Guenther reference clearly take place without any relationship to each other. It is not even necessary to rely on the teaching of a smart card in the Guenther reference for this purpose, since such separate printing processing takes place in the printer control 16 and all security-related processing takes place in the postal security module 86 in the Guenther reference. Independent claims 1 and 9 on appeal, however, require that the tasks relating to printing and the tasks relating to generating the security code, even though taking place in separate units, are interleaved. It is this interleaving which achieves the aforementioned timesavings.

Since at least in the Windel et al. ;463 reference, such processing of printing tasks and security-related tasks takes place fundamentally in the same manner as in Guenther, modifying the Windel et al reference in accordance with the teachings of Guenther would result in virtually no changes at all to the operation of the Windel et

al system, at least one the basis of how and where these different types of processing take place.

In view of the complete absence in any of these references to divide and then, to a certain extent, interleave these different processing tasks in any of the references cited by the Examiner, Appellants respectfully submit that there is no motivation to modify those references, in any combination, to arrive at an arrangement as set forth in independent claim 1 or a method as forth in independent claim 9. Appellants therefore submit that the subject matter of claims 1 and 9-11 would not have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) based on the teachings of these references.

In responding to these arguments, the Examiner in the final rejection stated that Appellants are basing their arguments in support of patentability on a separation of tasks between two data processing units, namely a security module and a print module. The Examiner stated the pre-calculation task of the first processor is a set of pre-calculations to calculate a constant number that does not change as the mail pieces are run through the system, the only variable being the count that would change according to the mail piece. The Examiner further stated that the fact that a division of tasks does, in fact, speed up a process is well known in the art, and that it is inherent that if a task is divided among a number of processors, it will take less time to achieve certain results. The Examiner analogized this situation to the holding of the CCPA in *In re Dulberg*, 129 U.S.P.Q. 348, 349 (CCPA 1961), that it is not invention to merely make various parts separable without unexpected results if access to something is desirable.

As Appellants' argument above makes clear, it is true that Appellants are relying on the separation of the tasks respectively performed for generating and printing the security imprint and generating and printing the other print data in the image as a basis for patentability. Appellants, however, are not "merely" relying on this feature. Appellants submit that before it can even be determined whether the division of an overall processing procedure into multiple, separately-conducted procedures has any benefit, one must first ascertain exactly how the overall procedure will be divided. Appellants respectfully submit it is not always the case, and not always clear in advance, that such a division necessarily will improve processing or always be desirable. Moreover, even if such a division has the possibility of improving processing, the associated costs may be prohibitive so that the benefit in improving processing speed is offset by the added costs so as to cause the division to be untenable or unpractical.

Assessing the patentability of the claims on appeal by simply asking whether it would have been obvious to perform tasks relating to printing the security imprint separately from tasks relating to the printing of other data in the overall image, therefore, begs the question of obviousness. Before one can assess the obviousness of separately performing these tasks, the non-obviousness of identifying and separately performing the tasks associated with printing the security imprint must be assessed. There are many other ways by which the overall printing process can be divided, and not all of those possibilities involve separating out the tasks relating to printing the security imprint. This is analogous to the numerous decisions which exist which state that recognition of the source of a problem is a relevant factor to be taken into consideration in the overall assessment of

obviousness or non-obviousness. The first step in the procedure which resulted in the subject matter of the claims on appeal was to decide how the overall printing procedure should be divided to attain the benefit of improved throughput. The inventors' first step was to have the insight that separating out the tasks relating to printing the security imprint could have benefit to achieve this goal. None of the references relied upon by the Examiner provide any teaching or insight that this is so, or even that this could be so. There is no discussion in any of those references regarding a need, or even a desire, to relieve the burden on the processor which must print a print image containing a security imprint. Because such teachings are not contained in the references, there is no teaching that such relief can be obtained by separating out the tasks relating to printing the security imprint from the tasks related to printing the other data in the image. As stated in *Ex parte Campbell*, 211 U.S.P.Q. 575, 576 (PTO Bd. App. 1981):

> Although the solution to the problem would have been obvious once recognized, none of the prior art before us indicates any recognition of the existence of the problem.

Although the Appellants herein do not admit that once the appropriate division of tasks was decided upon, the remaining steps or components would have been obvious, it is clear that the references herein do not address this initial consideration, and therefore fail to substantiate the rejection under §103(a).

For similar reasons, Appellants respectfully submit that the Examiner's reliance on the *In re Dulberg* decision is inappropriate. As the Examiner acknowledged, that decision involved claims related to a mechanical device, wherein physical access to an interior component was desired. The claims on appeal in that decision required that one of the parts in the overall apparatus be removable from

another part in order to produce the access. The prior art taught that these two parts should be "press fitted" together. Therefore, the sole issue was where it would have been obvious, instead of "press fitting" the parts together, to make one part removable from the other. This decision does not present the same issue as the claims in the present appeal, however, because the prior art discussed in the decision already taught that the components in question were, or had to be, separate parts, and the only question was how those parts should be connected together (i.e., in "press fitted" fashion or in removable fashion). The *In re Dulberg* decision would be analogous to the present situation if the prior art in that decision had taught a single, unitary component which the inventor/appellant was claiming as being separated into two parts which were removable from each other. This would then be a situation analogous to a person of ordinary skill in the art being faced with the overall printing procedure and having to first decide, without any guidance from the references, as to whether and how the overall procedure should be separated to achieve the advantage of increased throughput. The references herein, by failing to address this basic issue, do not even provide guidance that taking such an approach would, in fact, improve throughput or increase the processing speed. The Examiner has cited instances where such a result does occur, however, those of ordinary skill in the relevant art are sophisticated enough to know that this will not always be the case.

The Examiner's basic combination of the teachings of Windel et al. '463, Gilham and Guenther thus fails to establish a *prima facie* case of obviousness for claims 1 and 9-11.

Claims 2-5 and 12-13 were rejected under 35 U.S.C. §103(a) as being unpatentable over the aforementioned combination, further in view of Eckert. Claim 5 was rejected based on this combination, further in view of Windel et al '146. Claims 7 and 8 were rejected over this last-mentioned combination, further in view of Cordery.

All of these rejections are traversed for the same reasons discussed above in connection with the rejection of claims 1 and 9-11. The Examiner has merely added further references to a combination which the Examiner already has acknowledged does not explicitly teach the organization of the processing tasks as set forth in claims 1 and 9. Moreover, although Appellants acknowledge that there is no limit t the number references which can be combined to allegedly substantiate a rejection under Section 103(a), their comes a point when so many references are combined that this is evidence of invention, rather than evidence of non-obviousness. It is clear that the Examiner has merely combed the art with the claims as a roadmap in an effort to locate each detail of the claimed subject matter. A person of ordinary skill in the art who has not had the benefit of first reading the present disclosure has no such guidance to instruct him or her through the large number of patents in this technology, and Appellants respectfully submit it is unrealistic to assume that such a person of ordinary skill in the art would be able to locate the "right" patents as the Examiner has done without first having had the benefit of reading Appellants' disclosure.

CONCLUSION:

For the foregoing reasons, Appellants respectfully submit the Examiner is in error in law and in fact in rejecting each of claims 1-14. Reversal of this rejection is therefore proper, and the same is respectfully requested.

This Appeal Brief is accompanied by a check in the amount of $320.00 for the requisite fee.

Submitted by,

Steven H. Noll (Reg. 28,982)

SCHIFF, HARDIN & WAITE
CUSTOMER NO. 26574
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Appellants.

CERTIFICATE OF MAILING

I hereby certify that an original and two copies of this correspondence are being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on July 1, 2003.

Steven H. Noll

STEVEN H. NOLL

APPENDIX "A"

1. An arrangement for generating a security imprint comprising:

a security module containing a first program memory in which a first program is stored and a security module data processing unit connected to said first program memory and being programmed by said first program to calculate a multi-byte security code from existing system data and to be able to receive new system data to modify said existing system data;

a separate data processing unit disposed externally of said security module and having a second program memory in which a second program is stored, said separate data processing unit being programmed by said second program to edit print data to compile a print image that contains said security code as a security imprint and that embodies a monetary value for franking a mail item; and

said security module data processing unit being further programmed by said first program to, immediately upon receipt of said new system data, validate said new system data and determine whether said new system data are required for said security code and, if so, to immediately begin recalculating said security code in a first routine and, in a second routine, to finish recalculating said security code for at least one security imprint, thereby producing a recalculated security code, and to initiate an accounting operation for said monetary value and to

communicate the recalculated security code to said separate data processing unit.

2. An arrangement as claimed in claim 1 wherein said security code is a data authorization code and wherein said security module data processing unit contains an internal non-volatile memory in which at least one key for calculating said data authorization code is protectively stored against access and wherein said security module contains a further security module data processing unit for performing said accounting.

3. An arrangement as claimed in claim 2 wherein said security module data processing unit is a processor programmed by said first program to calculate a first eight bytes of said data authorization code in advance in said first routine each day, and wherein said further security module data processing unit is a hardware accounting unit which produces an accounting result as a result of said accounting in said second routine, and wherein said security module further contains a non-volatile memory, accessible by said hardware accounting unit, in which said hardware accounting unit stores said accounting result.

4. An arrangement as claimed in claim 3 wherein said processor is programmed by said first program to determine an ascending register value, dependent on said monetary value, for at least one mail item, and to finish calculating said data authorization code in said second routine for said at least one mail item using said ascending register value.

5. An arrangement as claimed in claim 3 for use with a plurality of mail items all having the same monetary value for franking, and wherein said processor is programmed by said first program to pre-calculate a next-successive data

authorization code for a next mail item after debiting said monetary value for a preceding mail item, and to immediately communicate said next-successive data authorization code to said separate data processing unit.

6. An arrangement as claimed in claim 3 wherein said internal non-volatile memory is an SRAM of said processor, and wherein said security module further comprises a battery supporting said SRAM, and wherein said SRAM had memory areas for protected storage of at least some data produced by said pre-calculation, and wherein said at least one key for calculating said data authorization code is protectively stored in a memory area of said SRAM.

7. An arrangement as claimed in claim 6 wherein said processor is programmed by said first program to calculate said data authorization code using a machine identifier and OCR key indicator, a date, said monetary value, and a register value for an ascending register.

8. An arrangement as claimed in claim 2 wherein said processor is programmed by said first memory to calculate said data authorization code using an algorithm selected from the group consisting of DES algorithms and triplet DES algorithms.

9. A method for generating a security imprint, comprising the steps of:

providing a security module containing a security module data processing unit;

presetting all system data required for calculating a security code and, upon receipt of new system data requiring a re-calculation of the security code, in said security module data processing unit immediately

validating said new system data and re-calculating said security code using said new system data;

also in said security module data processing unit calculating an ascending register value for a monetary value associated with said new system data; and

communicating the re-calculated security code to a separate data processing unit external of said security module and compiling a print image, including said security code as a security imprint and printing said print image.

10. A method as claimed in claim 9 comprising calculating a data authorization code in said security module data processing unit as said security code dependent on said ascending register value and additional data in said new system data and generating said security imprint at a time following an end of entry of said new system data and before conducting an accounting for said monetary value.

11. A method as claimed in claim 9 wherein said new system data are associated with an inserted mail item and wherein said security code is a data authorization code and wherein said security module data processing unit calculates said data authorization code dependent on said ascending register value and additional data in said new system data at a time from said insertion of said mail item and before conducting an accounting for said monetary value.

12. A method as claimed in claim 9 wherein said security code is a data authorization code and wherein said security module data processing unit calculates said data authorization code dependent on a machine identifier, said monetary value and a current date, and wherein at least said machine identifier is included in a pre-calculation of n bytes of said data authorization code.

13. A method as claimed in claim 9 wherein said security code is a data authorization code and wherein said security module data processing unit calculates said data authorization code dependent on a machine identifier, said monetary value and a current date, and wherein at least said machine identifier and said date is included in a pre-calculation of n bytes of said data authorization code.

14. A method as claimed in claim 9 comprising successively supplying sets of new system data to said security module data processing unit and after communicating said security code to said separate data processing unit, in said security module data processing unit beginning calculation of a next-successive security code for next new system data, at least dependent on said ascending register value to produce pre-calculated n bytes of said next-successive security code.

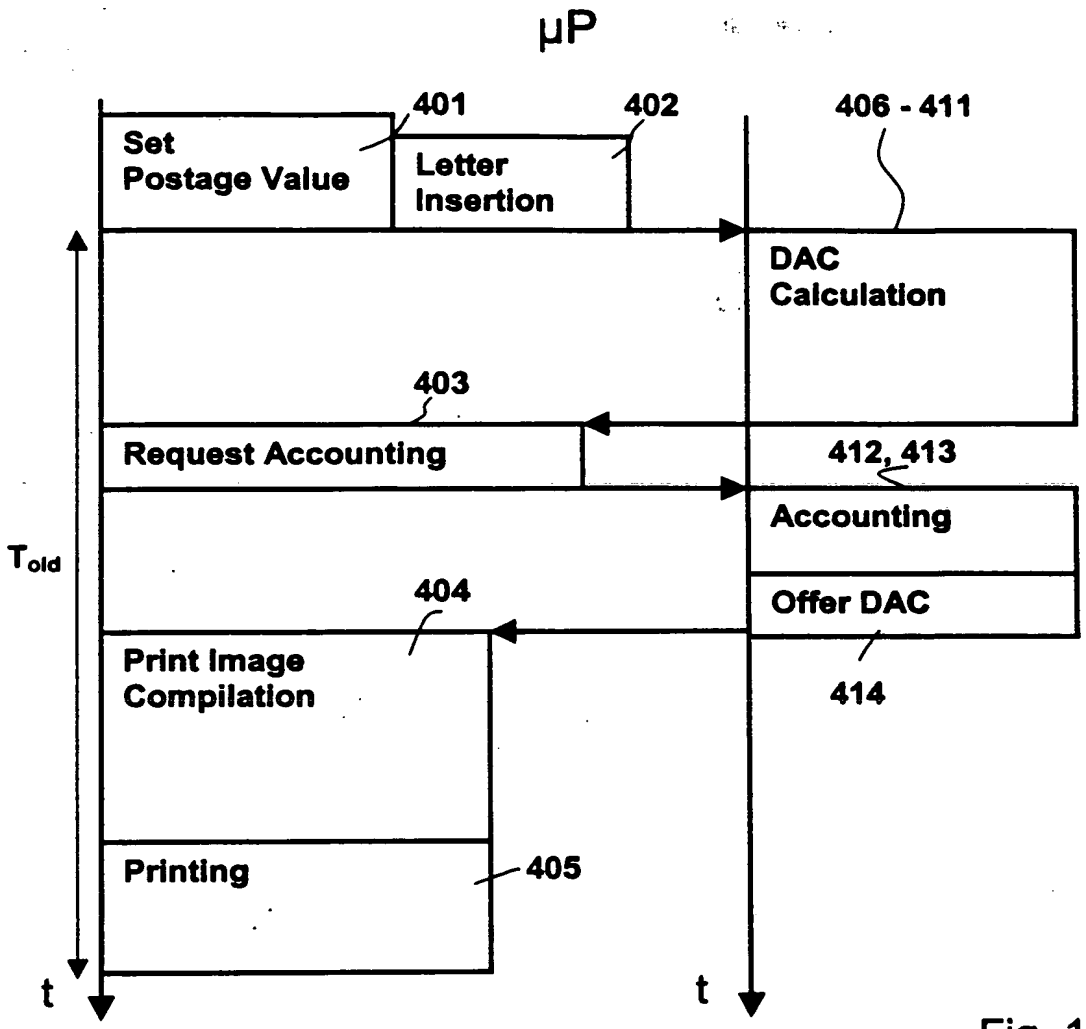
µP
401
402
406 - 411
Set Postage Value
Letter Insertion
DAC Calculation
403
Request Accounting
412, 413
Accounting
Offer DAC
404
Print Image Compilation
414
Printing
405
T_{old}
t
t

Fig. 1a

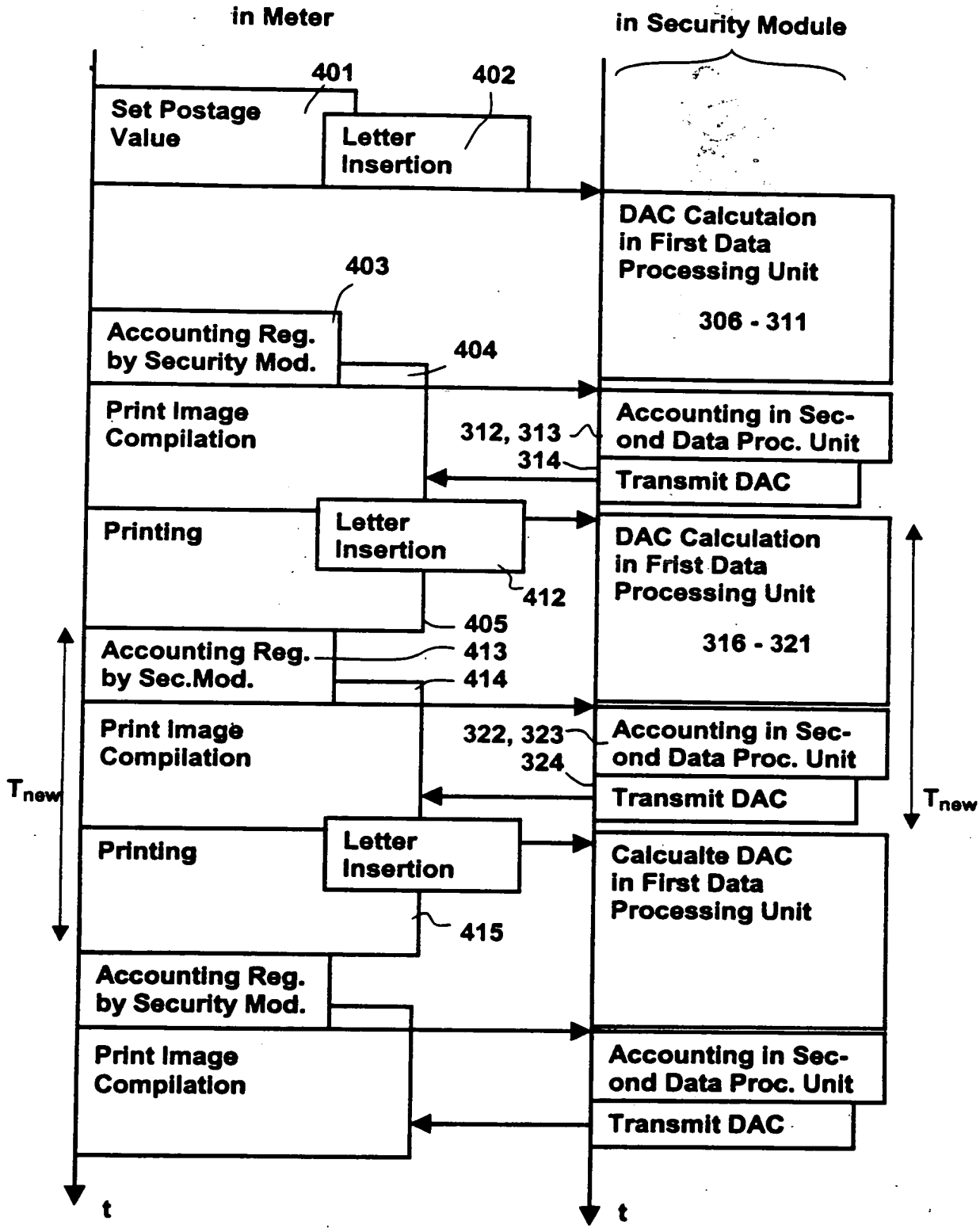
in Meter
in Security Module
401
402
Set Postage Value
Letter Insertion
DAC Calcutaion in First Data Processing Unit
306 - 311
403
Accounting Reg. by Security Mod.
404
Print Image Compilation
312, 313
Accounting in Second Data Proc. Unit
314
Transmit DAC
Printing
Letter Insertion
412
DAC Calculation in Frist Data Processing Unit
316 - 321
405
Accounting Reg. by Sec.Mod.
413
414
Print Image Compilation
322, 323
Accounting in Second Data Proc. Unit
324
Transmit DAC
Tnew
Tnew
Printing
Letter Insertion
Calcualte DAC in First Data Processing Unit
415
Accounting Reg. by Security Mod.
Print Image Compilation
Accounting in Second Data Proc. Unit
Transmit DAC
t
t

Fig. 1b

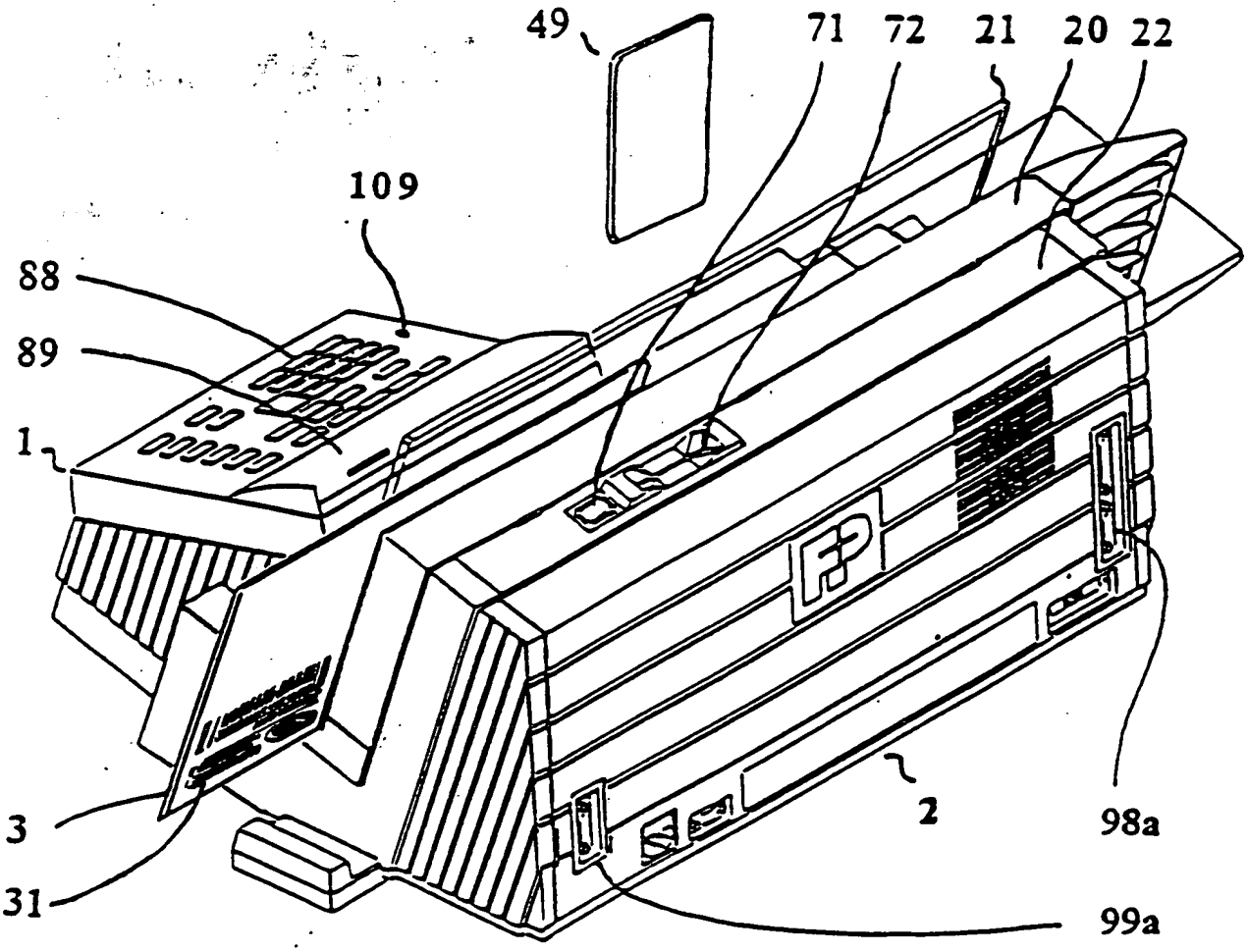
49
71
72
21
20
22
109
88
89
1
3
31
2
98a
99a

Fig. 3

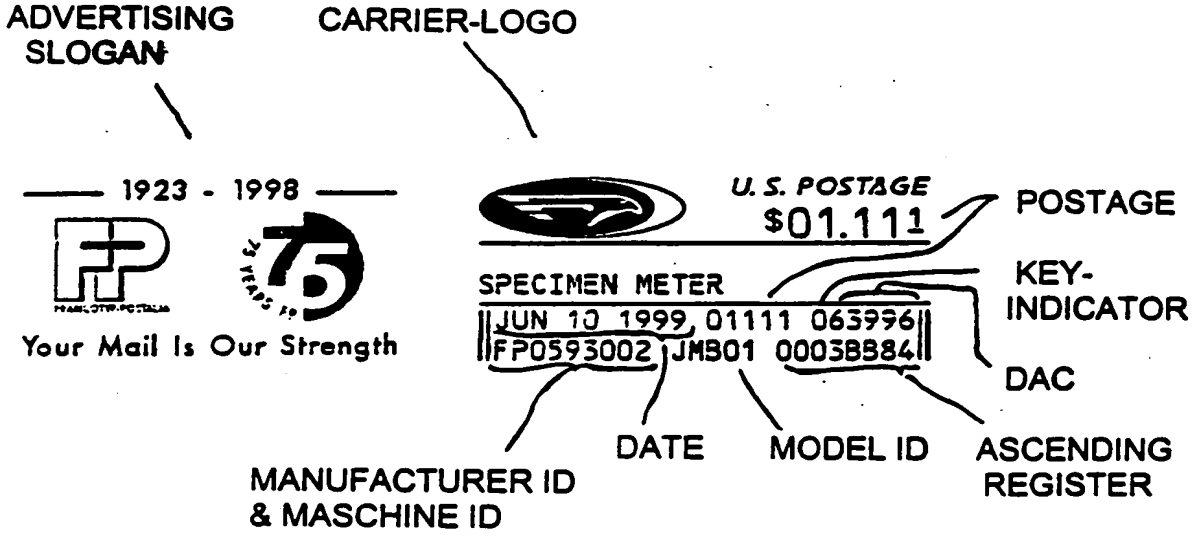
ADVERTISING SLOGAN
CARRIER-LOGO
1923 - 1998
Your Mail Is Our Strength
U.S. POSTAGE
$01.111
POSTAGE
SPECIMEN METER
JUN 10 1999 01111 063996
FP0593002 JMB01 00038884
KEY-INDICATOR
DAC
MANUFACTURER ID & MASCHINE ID
DATE
MODEL ID
ASCENDING REGISTER

Fig. 4